INFORMATION TECHNOLOGY UNIVERSITY

Blockchain

Assignment Report

Small Contracts

Course Instructor

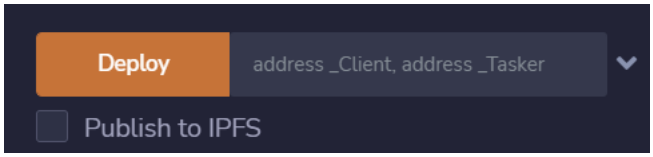
Dr Umar Janjua

Submitted by

Muhammad Taqi Raza (Bscs20031)

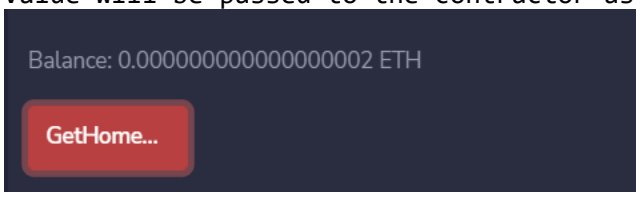
Task 1

Here we will have two addresses Client and Tasker. The addresses will be passed through constructors while deploying the contract.



The functions using are below, here I am not mentioning the body of the functions,

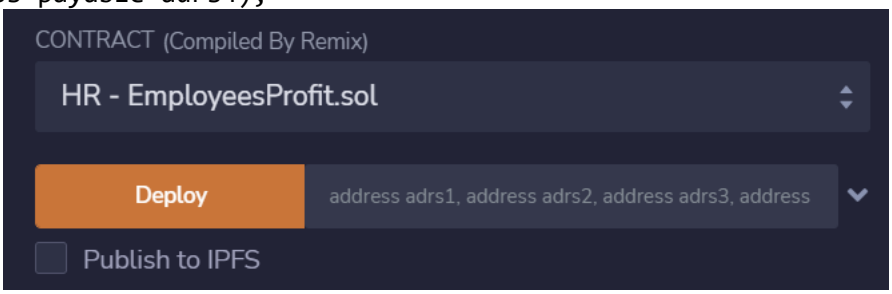
```
function GetHomeService()public payable;
This function can only be called by the Client. As Client call this function with
payment the payment Value will be passed to the contractor as shown
```

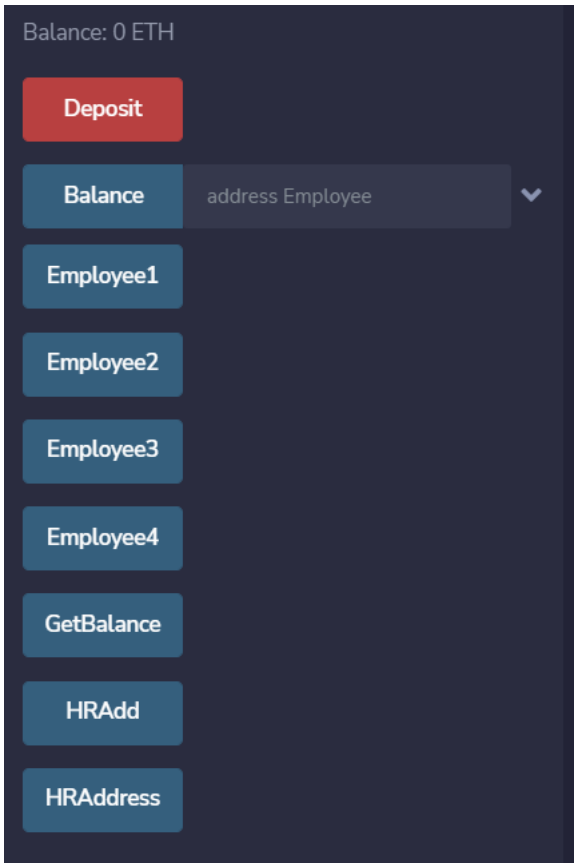



```
function TaskDoneByTasker() public;
This function can be called by the Tasker to inform client that he has done the
task.

function TaskToApprove()public;
After the task done by the tasker it needs to be approved by the Client as Client
approve the task the payment will be transferred to the tasker

function getBalance() public view returns (uint)
This function returns the balance in the contract.
```

Task 2

```
We will pass the addresses of the employees in the constructor
constructor(address payable adrs1,address payable adrs2,address payable
adrs3,address payable adrs4);
```

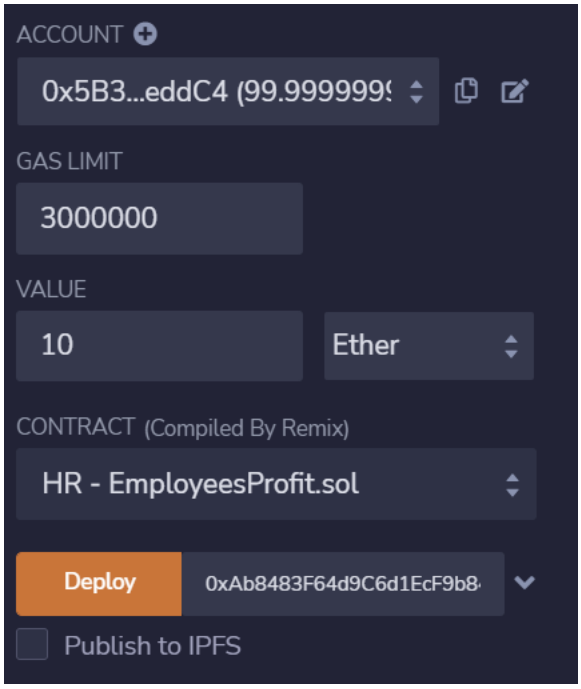




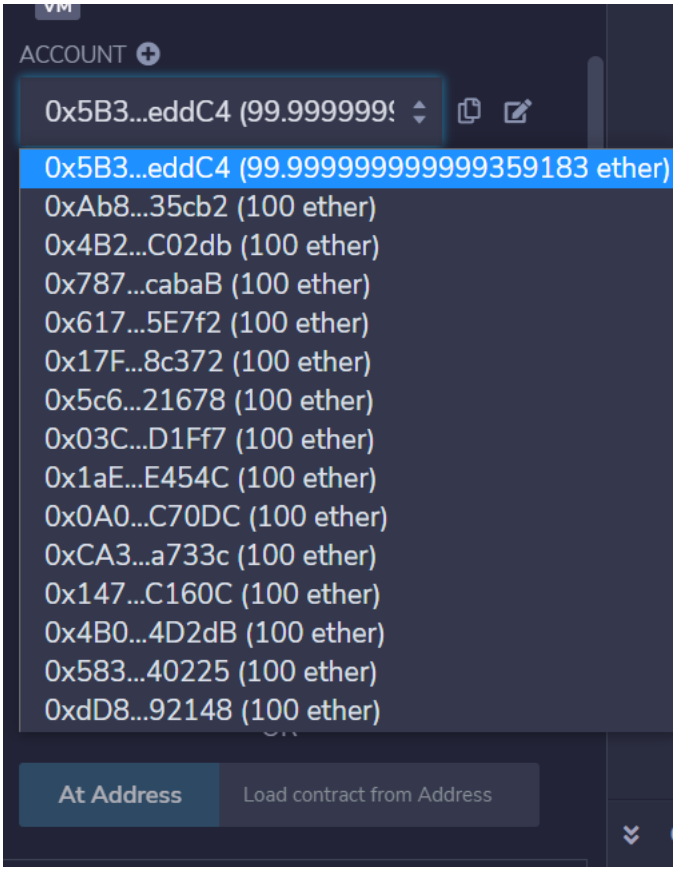
function Deposit() public payable OnlyHR;
This payable function will get the payment and distribute it to the employees according to the percentage assigned.
This function can only be called by the HR.

modifier OnlyHR()
This modifier checks that Only HR can deposit to the employees.

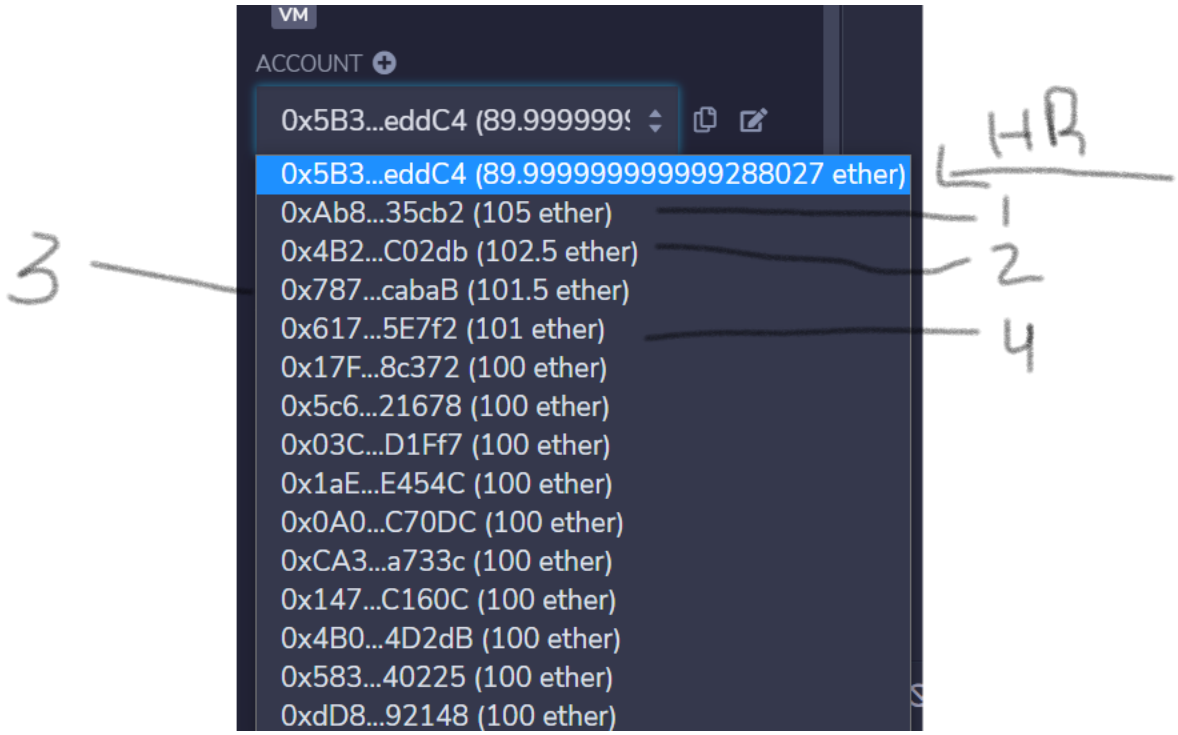
The HR is going to Deposit 10 ethers to the employees following the percentages.



Before Depositing



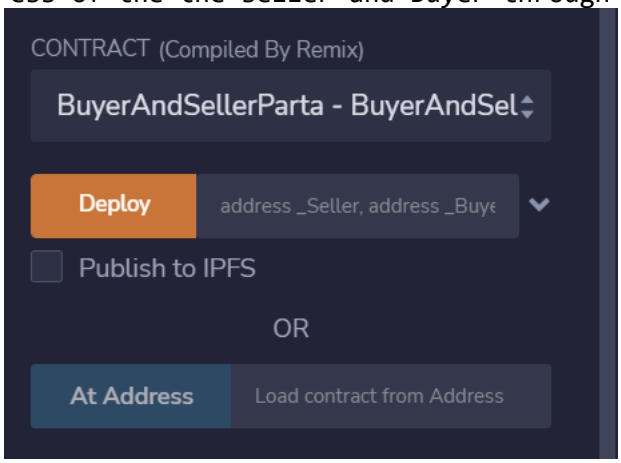
After depositing we have,



Task 3

(a)

We will pass the address of the the seller and Buyer through the constructor;

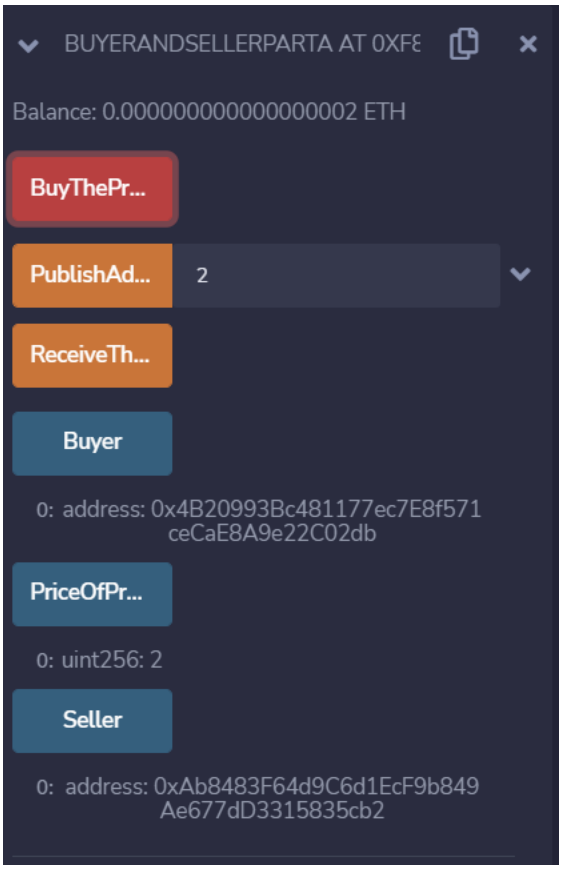



```
constructor(address payable _Seller,address payable _Buyer);
function PublishAdvertisement(uint Price) public
```

Publish Advertisement is the function that will be only called by the Seller and he will pass the price of the product.

```
function BuyTheProduct() payable public
```

This function will be called by the buyer with the value passing as a payment to the contractor.




```
function ReceiveTheProductConfirmation() public
```

As a buyer receives the product he will call this function and the payment will released to the seller.

Security Issues

So the main security reason here is that if the buyer receives the product may be he will not confirms that he have receive the product or not and the payment will not be released to the seller.

Task 3

(b)

So to resolve the issue that buyer must confirm that he receive the product we have an idea that seller will deposit 2X of the price of product and buyer will also deposit the 2X of the price of the product.

Means that if the Price of the product = 2 gwei

Amount deposited by Seller= 4 gwei

Amount deposited by buyer= 4 gwei

Total deposited value in the contract = 8 gwei

So at this time buyer has his 2 gwei in the contract and seller has 6 gwei in the contract (4gwei he deposited + 2gwei the price of which he sell his product).

After the buyer receives the product to get his 2 gwei back he will have to confirm that he receives the product and as a result of this confirmation seller will get his 6 gwei.

```
function ReceiveTheProductConfirmation() public
{
    require(msg.sender==Buyer,"Only Buyer can confirm that he have Received The product");
    require(has_Shipped==true,"Product has not been shipped");
    require(has_Shipped==true,"Product has not been shipped");

    uint256 amountDeposited=address(this).balance;
    Seller.transfer(amountDeposited*3/4);
    Buyer.transfer(amountDeposited*1/4);

    MessagePublished=false;
    PriceOfProduct=2;
    has_Shipped=false;

}
```

So in this way we had insured the security from both sides.